Polos Olímpicos de Treinamento

Curso de Teoria dos Números - Nível 3

Carlos Gustavo Moreira

Aula 9

Congruências de grau 2 e reciprocidade quadrática

1 Congruências de Grau 2

Seja $p > 2$ um número primo e $a, b, c \in \mathbb{Z}$ com a não divisível por p. Resolver a equação quadrática

$$ax^2 + bx + c \equiv 0 \pmod{p}$$

é o mesmo que resolver (completando quadrados)

$$(2ax + b)^2 \equiv b^2 - 4ac \pmod{p}$$

(note que 2 e a são invertíveis módulo p). Assim, estamos interessados em encontrar critérios de existência de soluções da equação

$$X^2 \equiv d \pmod{p}.$$

Se a equação acima admite solução (i.e. se $\overline{d}$ é um "quadrado perfeito" em $\mathbb{Z}/p\mathbb{Z}$) então dizemos que d é um *resíduo ou resto quadrático* módulo p. Há exatamente $(p+1)/2$ resíduos quadráticos módulo p, a saber

$$0^2, 1^2, 2^2, 3^2, \ldots, \left(\frac{p-1}{2}\right)^2 \bmod p$$

já que todo inteiro x é congruente a $\pm i \bmod p$ para algum i tal que $0 \leq i \leq (p-1)/2$, de modo que x^2 é congruente a um dos números da lista acima. Note que módulo p estes números são todos distintos: de fato, temos que

$$\begin{aligned} i^2 \equiv j^2 \pmod{p} &\implies p \mid (i-j)(i+j) \\ &\iff p \mid i-j \text{ ou } p \mid i+j \\ &\iff i \equiv \pm j \pmod{p} \end{aligned}$$

Mas como $0 \leq i, j \leq (p-1)/2 \implies 0 < i + j \leq p - 1$ ou $i = j = 0$, temos que a única possibilidade é $i \equiv j \pmod{p}$.

Embora saibamos a lista completa dos resíduos quadráticos, na prática pode ser difícil reconhecer se um número é ou não resíduo quadrático. Por exemplo, você sabe dizer se 2 é resíduo quadrático módulo 1019? Veremos a seguir o teorema da reciprocidade quadrática, que permite responder estas questões de maneira bastante eficiente.

1.1 Resíduos Quadráticos e Símbolo de Legendre

Seja $p > 2$ um número primo e a um inteiro qualquer. Para simplificar cálculos e notações definiremos o chamado *símbolo de Legendre*:

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{se } p \nmid a \text{ e } a \text{ é um resíduo quadrático módulo } p \\ 0 & \text{se } p \mid a \\ -1 & \text{caso contrário} \end{cases}$$

Proposição 1 (Critério de Euler). *Seja $p > 2$ um primo e a um inteiro qualquer. Então*

$$\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod{p}.$$

Demonstração. Para $a \equiv 0 \pmod{p}$ o resultado é claro, de modo que podemos supor $p \nmid a$. Pelo teorema de Fermat temos que $a^{p-1} \equiv 1 \pmod{p}$, donde

$$\begin{aligned}(a^{\frac{p-1}{2}} - 1)(a^{\frac{p-1}{2}} + 1) \equiv 0 \pmod{p} &\iff p \mid a^{\frac{p-1}{2}} - 1 \text{ ou } p \mid a^{\frac{p-1}{2}} + 1 \\ &\iff a^{\frac{p-1}{2}} \equiv \pm 1 \pmod{p}.\end{aligned}$$

Assim, devemos mostrar que $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$ se, e só se, a é um resíduo quadrático módulo p.

Se a é um resíduo quadrático, digamos $a \equiv i^2 \pmod{p}$, novamente pelo teorema de Fermat temos que

$$a^{\frac{p-1}{2}} \equiv i^{p-1} \equiv 1 \pmod{p}.$$

Assim, os resíduos quadráticos $1^2, 2^2, \ldots, (\frac{p-1}{2})^2$ módulo p são raízes do polinômio $f(x) = x^{\frac{p-1}{2}} - \overline{1}$ em $\mathbb{Z}/(p)[x]$. Mas $\mathbb{Z}/(p)$ é corpo, logo $f(x)$ pode ter no máximo $\deg f = (p-1)/2$ raízes em $\mathbb{Z}/(p)$. Isto mostra que as raízes de $f(x)$ são exatamente os resíduos quadráticos não congruentes a zero módulo p e que, portanto, $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$ se, e só se, a é um resíduo quadrático módulo p. □

Corolário 2. *O símbolo de Legendre possui as seguintes propriedades:*

1. *se $a \equiv b \pmod{p}$ então $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.*
2. *$\left(\frac{a^2}{p}\right) = 1$ se $p \nmid a$.*
3. *$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$, ou seja, -1 é resíduo quadrático módulo p se, e só se, $p \equiv 1 \pmod{4}$.*
4. *$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$.*

Demonstração. Os itens *1* e *2* são imediatos a partir da definição e *3* segue do critério de Euler: $\left(\frac{-1}{p}\right) \equiv (-1)^{\frac{p-1}{2}} \pmod{p} \implies \left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$ já que $p > 2$

e ambos os lados da congruência são iguais a ± 1. Da mesma forma, aplicando o critério de Euler temos que

$$\left(\frac{ab}{p}\right) \equiv (ab)^{\frac{p-1}{2}} \equiv a^{\frac{p-1}{2}} b^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \pmod{p},$$

o que mostra que $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$, pois novamente ambos os lados da congruência são iguais a ± 1. □

Exemplo 3. *Mostre que o polinômio $f(x) = x^4 - 10x^2 + 1$ é irredutível em $\mathbb{Z}[x]$, mas é redutível módulo p para todo primo p.*

Solução: Vejamos que $f(x)$ é irredutível em $\mathbb{Z}[x]$. Observe inicialmente que as raízes de $f(x)$ são todas irracionais: se $p, q \in \mathbb{Z}$ são tais que $\text{mdc}(p, q) = 1$ e $f(p/q) = 0 \iff p^4 - 10p^2q^2 + q^4 = 0$, temos da última igualdade que $q \mid p^4 \implies q = \pm 1$ e $p \mid q^4 \implies p = \pm 1$ já que p e q são primos entre si, logo $p/q = \pm 1$, nenhuma das quais é raiz de $f(x)$ (cujos zeros são $\pm\sqrt{2} \pm \sqrt{3}$).

Logo se $f(x)$ for redutível ele é o produto de dois polinômios de grau 2, que podemos supor mônicos. Como o produto dos coeficientes independentes destes dois fatores deve ser igual ao coeficiente independente de $f(x)$, que é 1, temos apenas duas possibilidades:

$$f(x) = (x^2 + ax + 1)(x^2 + bx + 1) \qquad \text{ou}$$
$$f(x) = (x^2 + ax - 1)(x^2 + bx - 1)$$

com $a, b \in \mathbb{Z}$. Em ambos os casos, temos $a + b = 0$ (coeficiente de x^3). Logo, no primeiro caso, comparando o coeficiente de x^2 temos $ab + 2 = -10 \iff a^2 = 12$, o que é impossível. O segundo caso é análogo.

Agora, para $p = 2$ e $p = 3$ temos

$$f(x) \equiv (x + 1)^4 \pmod{2} \qquad \text{e} \qquad f(x) \equiv (x^2 + 1)^2 \pmod{3}.$$

Agora se $p > 3$ é um primo, temos que ou $\left(\frac{2}{p}\right) = 1$, ou $\left(\frac{3}{p}\right) = 1$ ou $\left(\frac{6}{p}\right) = 1$ já que $\left(\frac{2}{p}\right)\left(\frac{3}{p}\right) = \left(\frac{6}{p}\right)$. No primeiro caso, se $a^2 \equiv 2 \pmod{p}$ temos

$$f(x) \equiv (x^2 + 2ax - 1)(x^2 - 2ax - 1) \pmod{p}.$$

Já no segundo caso, se $b^2 \equiv 3 \pmod{p}$ temos

$$f(x) \equiv (x^2 + 2bx + 1)(x^2 - 2bx + 1) \pmod{p}.$$

Finalmente, no último caso, se $c^2 \equiv 6 \pmod{p}$ temos

$$f(x) \equiv (x^2 + 2c - 5)(x^2 - 2c - 5) \pmod{p}.$$

Isto mostra que $f(x)$ é redutível módulo p para todo primo p. □

1.2 Lei de Reciprocidade Quadrática

O critério de Euler já nos fornece uma maneira de identificar resíduos quadráticos. Entretanto, vamos provar um resultado muito mais forte, que é a famosa

Teorema 4 (Reciprocidade Quadrática)**.**

1. *Sejam p e q primos ímpares distintos. Então*
$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}.$$
2. *Seja p um primo ímpar. Então*
$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = \begin{cases} 1 & \text{se } p \equiv \pm 1 \pmod 8 \\ -1 & \text{se } p \equiv \pm 3 \pmod 8. \end{cases}$$

Antes de apresentar a prova, vejamos algumas aplicações.

Exemplo 5. *Determinar se -90 é resíduo quadrático módulo 1019 ou não.*

Solução:

$$\begin{aligned}\left(\frac{-90}{1019}\right) &= \left(\frac{-1}{1019}\right)\left(\frac{2}{1019}\right)\left(\frac{3^2}{1019}\right)\left(\frac{5}{1019}\right) \\ &= (-1)\cdot(-1)\cdot 1\cdot\left(\frac{1019}{5}\right) \\ &= \left(\frac{4}{5}\right) = \left(\frac{2^2}{5}\right) = 1.\end{aligned}$$

Ou seja, -90 é resíduo quadrático módulo 1019. □

Exemplo 6. *Seja p um número primo. Mostre que*

1. *se p é da forma $4n+1$ então $p \mid n^n - 1$.*
2. *se p é da forma $4n-1$ então $p \mid n^n + (-1)^{n+1}\cdot 2n$.*

Solução: No primeiro item, $4n \equiv -1 \pmod p$, donde elevando a n obtemos

$$(4n)^n = 2^{2n}n^n \equiv (-1)^n \pmod p.$$

Por outro lado, pelo critério de Euler e pela reciprocidade quadrática temos

$$2^{2n} = 2^{\frac{p-1}{2}} \equiv (-1)^{\frac{p^2-1}{8}} \equiv (-1)^{n(2n+1)} \equiv (-1)^n \pmod p.$$

Portanto $n^n \equiv 1 \pmod p$, como queríamos demonstrar.

No segundo item, temos $4n \equiv 1 \pmod p$ e assim

$$(4n)^n = 2^{2n}n^n \equiv 1 \pmod p,$$

mas $2^{2n-1} = 2^{\frac{p-1}{2}} \equiv (-1)^{\frac{p^2-1}{8}} = (-1)^{n(2n-1)} \pmod p$, donde $2^{2n} \equiv 2\cdot(-1)^n \pmod p$. Concluímos que $2n^n \equiv (-1)^n \pmod p$ e multiplicando por $2n$ e utilizando $4n \equiv 1 \pmod p$ obtemos $n^n \equiv 2n\cdot(-1)^n \pmod p$, como desejado. □

O primeiro passo da demonstração da lei de reciprocidade quadrática é o seguinte

Lema 7 (Gauß). *Sejam $p > 2$ um número primo e a um inteiro positivo primo relativo com p. Seja s o número de elementos do conjunto*

$$\left\{a, 2a, 3a, \ldots, \tfrac{p-1}{2} \cdot a\right\}$$

tais que seu resto módulo p é maior do que $\frac{p-1}{2}$. Então

$$\left(\frac{a}{p}\right) = (-1)^s.$$

Demonstração. A ideia é imitar a prova do teorema de Euler-Fermat. Como o conjunto $\{\pm 1, \pm 2, \ldots, \pm\frac{p-1}{2}\}$ é um sistema completo de invertíveis módulo p, para cada $j = 1, 2, \ldots, \frac{p-1}{2}$ podemos escrever $a \cdot j \equiv \epsilon_j m_j \pmod{p}$ com $\epsilon_j \in \{-1, 1\}$ e $m_j \in \{1, 2, \ldots, \frac{p-1}{2}\}$. Temos que se $i \neq j$ então $m_i \neq m_j$ donde $\{m_1, m_2, \ldots, m_{\frac{p-1}{2}}\} = \{1, 2, \ldots, \frac{p-1}{2}\}$. De fato, se $m_i = m_j$ temos $a \cdot i \equiv a \cdot j \pmod{p}$ ou $a \cdot i \equiv -a \cdot j \pmod{p}$; como a é invertível módulo p e $0 < i, j \leq (p-1)/2$, temos que a primeira possibilidade implica $i = j$ e a segunda é impossível. Assim, multiplicando as congruências $a \cdot j \equiv \epsilon_j m_j \pmod{p}$, obtemos

$$\begin{aligned}(a \cdot 1)(a \cdot 2) \cdots (a \cdot \tfrac{p-1}{2}) &\equiv \epsilon_1 \epsilon_2 \cdots \epsilon_{\frac{p-1}{2}} m_1 m_2 \cdots m_{\frac{p-1}{2}} \pmod{p} \\ a^{\frac{p-1}{2}} \left(\frac{p-1}{2}\right)! &\equiv \epsilon_1 \epsilon_2 \cdots \epsilon_{\frac{p-1}{2}} \left(\frac{p-1}{2}\right)! \pmod{p} \\ \iff \left(\frac{a}{p}\right) &\equiv \epsilon_1 \epsilon_2 \ldots \epsilon_{\frac{p-1}{2}} \pmod{p},\end{aligned}$$

donde $(\frac{a}{p}) = \epsilon_1 \epsilon_2 \ldots \epsilon_{\frac{p-1}{2}}$, pois ambos os lados pertencem a $\{-1, 1\}$. Assim, $(\frac{a}{p}) = (-1)^s$ já s é o número de elementos j de $\{1, 2, \ldots, \frac{p-1}{2}\}$ tais que $\epsilon_j = -1$. □

O lema de Gauß já nos permite provar a fórmula para $\left(\frac{2}{p}\right)$. Se $p \equiv 1 \pmod{4}$, digamos $p = 4k + 1$, temos $\frac{p-1}{2} = 2k$. Como $1 \leq 2j \leq \frac{p-1}{2}$ para $j \leq k$ e $\frac{p-1}{2} < 2j \leq p - 1$ para $k + 1 \leq j \leq 2k$, temos

$$\left(\frac{2}{p}\right) = (-1)^k = \begin{cases} 1, & \text{se } p \equiv 1 \pmod{8}, \\ -1, & \text{se } p \equiv 5 \pmod{8}. \end{cases}$$

Se $p \equiv 3 \pmod{4}$, digamos $p = 4k + 3$, temos $\frac{p-1}{2} = 2k + 1$. Para $1 \leq j \leq k$ temos $1 \leq 2j \leq \frac{p-1}{2}$ e para $k + 1 \leq j \leq 2k + 1$ temos $\frac{p-1}{2} < 2j \leq p - 1$, donde

$$\left(\frac{2}{p}\right) = (-1)^{k+1} = \begin{cases} -1, & \text{se } p \equiv 3 \pmod{8}, \\ 1, & \text{se } p \equiv 7 \pmod{8}. \end{cases}$$

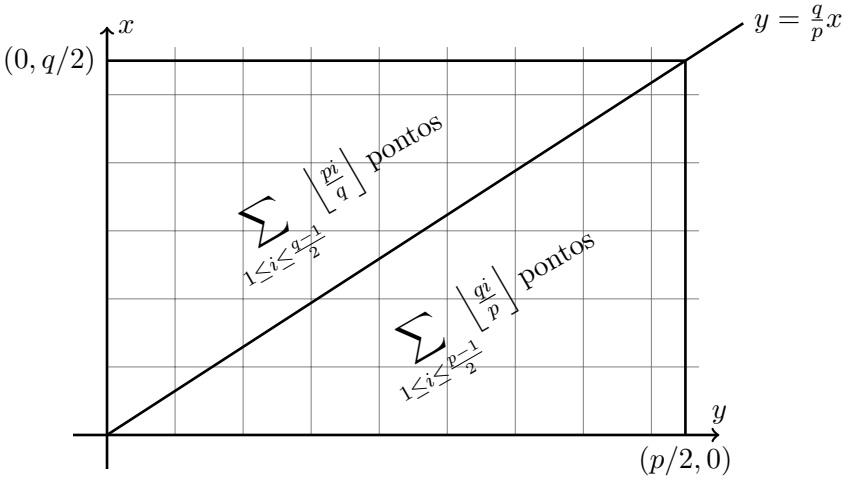
Agora, para provar o item *1* da lei de reciprocidade quadrática, vamos mostrar que

$$\frac{p-1}{2} \cdot \frac{q-1}{2} = \sum_{1 \leq i \leq \frac{q-1}{2}} \left\lfloor \frac{ip}{q} \right\rfloor + \sum_{1 \leq i \leq \frac{p-1}{2}} \left\lfloor \frac{iq}{p} \right\rfloor \qquad (*)$$

e que

$$\left(\frac{p}{q}\right) = (-1)^{\sum_{1\le i\le \frac{q-1}{2}} \left\lfloor \frac{ip}{q} \right\rfloor} \qquad \text{e} \qquad \left(\frac{q}{p}\right) = (-1)^{\sum_{1\le i\le \frac{p-1}{2}} \left\lfloor \frac{iq}{p} \right\rfloor}. \qquad (**)$$

A fórmula $(*)$ é apenas uma contagem: o lado esquerdo é o número de pontos com ambas as coordenadas inteiras no interior do retângulo de vértices $(0,0)$, $(p/2,0)$, $(0,q/2)$ e $(p/2,q/2)$.



Por outro lado, o primeiro somatório do lado direito conta o número de tais pontos que estão acima da diagonal $x = \frac{p}{q}y$ do retângulo, enquanto o segundo somatório conta o número de tais pontos abaixo desta diagonal (note que como p e q são primos, não há pontos com ambas as coordenadas inteiras na diagonal). Por exemplo, no primeiro somatório cada termo $\left\lfloor \frac{ip}{q} \right\rfloor$ representa a quantidade de pontos na reta $y = i$ acima da diagonal $x = \frac{p}{q}y$.

Finalmente, para mostrar $(**)$, basta checar que $\sum_{1\le i\le \frac{p-1}{2}} \left\lfloor \frac{iq}{p} \right\rfloor \equiv s \pmod 2$, onde s é como no lema de Gauß aplicado para $a = q$. Seja r_i o resto da divisão de iq por p, de modo que $iq = \left\lfloor \frac{iq}{p} \right\rfloor p + r_i$. Somando e utilizando a notação da demonstração do lema de Gauß, obtemos

$$q \sum_{1\le i\le \frac{p-1}{2}} i = p \sum_{1\le i\le \frac{p-1}{2}} \left\lfloor \frac{iq}{p} \right\rfloor + \sum_{r_i<p/2} m_i + \sum_{r_i>p/2} (p - m_i).$$

Como p e q são ímpares, módulo 2 temos

$$\sum_{1\le i\le \frac{p-1}{2}} i \equiv \sum_{1\le i\le \frac{p-1}{2}} \left\lfloor \frac{iq}{p} \right\rfloor + \sum_{r_i<p/2} m_i + \sum_{r_i>p/2} (1 + m_i) \pmod 2,$$

e como $\{m_1, m_2, \ldots, m_{\frac{p-1}{2}}\} = \{1, 2, \ldots, \frac{p-1}{2}\}$, concluímos assim que

$$\sum_{1\le i\le \frac{p-1}{2}} i \equiv \sum_{1\le i\le \frac{p-1}{2}} \left\lfloor \frac{iq}{p} \right\rfloor + \sum_{1\le i\le \frac{p-1}{2}} i + \sum_{r_i>p/2} 1 \pmod 2$$

$$\iff \sum_{1\le i\le \frac{p-1}{2}} \left\lfloor \frac{iq}{p} \right\rfloor \equiv s \pmod 2$$

o que encerra a prova.

Observação 8. *O símbolo de Legendre* $\left(\frac{a}{p}\right)$ *pode ser estendido para o símbolo de Jacobi* $\left(\frac{a}{n}\right)$*, que está definido para* a *inteiro arbitrário e* n *inteiro positivo ímpar por* $\left(\frac{a}{n}\right) = \left(\frac{a}{p_1}\right)^{\alpha_1}\left(\frac{a}{p_2}\right)^{\alpha_2}\ldots\left(\frac{a}{p_k}\right)^{\alpha_k}$ *se* $n = p_1^{\alpha_1}p_2^{\alpha_2}\ldots p_k^{\alpha_k}$ *é a fatoração prima de* n *(onde os* $\left(\frac{a}{p_j}\right)$ *são dados pelo símbolo de Legendre usual); temos* $\left(\frac{a}{1}\right) = 1$ *para todo inteiro* a*. Não é difícil provar as seguintes propriedades do símbolo de Jacobi, que podem ser usadas para calcular rapidamente símbolos de Legendre (e de Jacobi):*

1. *Se* $a \equiv b \pmod{n}$ *então* $\left(\frac{a}{n}\right) = \left(\frac{b}{n}\right)$.
2. $\left(\frac{a}{n}\right) = 0$ *se* $\mathrm{mdc}(a,n) \neq 1$ *e* $\left(\frac{a}{n}\right) \in \{-1,1\}$ *se* $\mathrm{mdc}(a,n) = 1$.
3. $\left(\frac{ab}{n}\right) = \left(\frac{a}{n}\right)\left(\frac{b}{n}\right)$*; em particular,* $\left(\frac{a^2}{n}\right) \in \{0,1\}$.
4. $\left(\frac{a}{mn}\right) = \left(\frac{a}{m}\right)\left(\frac{a}{n}\right)$*; em particular,* $\left(\frac{a}{n^2}\right) \in \{0,1\}$.
5. *Se* m *e* n *são positivos e ímpares, então* $\left(\frac{m}{n}\right) = (-1)^{\frac{m-1}{2}\cdot\frac{n-1}{2}}\left(\frac{n}{m}\right)$.
6. $\left(\frac{-1}{n}\right) = (-1)^{\frac{n-1}{2}}$.
7. $\left(\frac{2}{n}\right) = (-1)^{\frac{n^2-1}{8}}$.

Os três últimos fatos, que generalizam a lei de reciprocidade quadrática, podem ser provados usando a multiplicatividade em a *e em* n *do símbolo de Jacobi* $\left(\frac{a}{n}\right)$ *e a lei de reciprocidade quadrática para o símbolo de Legendre.*

Como para o símbolo de Legendre, se $\left(\frac{a}{n}\right) = -1$*,* a *não é resíduo quadrático módulo* n*, mas (diferentemente do que acontece para o símbolo de Legendre) é possível que* $\left(\frac{a}{n}\right)$ *seja igual a* 0 *ou a* 1 *sem que* a *seja resíduo quadrático módulo* n*. Por exemplo,* $\left(\frac{2}{15}\right) = \left(\frac{2}{3}\right)\left(\frac{2}{5}\right) = (-1)\cdot(-1) = 1$ *e* $\left(\frac{3}{15}\right) = \left(\frac{3}{3}\right)\left(\frac{3}{5}\right) = 0\cdot(-1) = 0$*, mas* 2 *e* 3 *não são resíduos quadráticos módulo* 15.

Problemas Propostos

Problema 9. *Calcular* $\left(\frac{44}{103}\right)$, $\left(\frac{-60}{1019}\right)$ *e* $\left(\frac{2010}{1019}\right)$.

Problema 10. *Determine todas as soluções de* $x^{10} \equiv 1 \pmod{49}$.

Problema 11. *Sejam* p *um primo ímpar e* c *um inteiro que não é múltiplo de* p*. Prove que*

$$\sum_{a=0}^{p-1}\left(\frac{a(a+c)}{p}\right) = -1.$$

Problema 12. *Existem inteiros* m *e* n *tais que*

$$5m^2 - 6mn + 7n^2 = 1985\ ?$$

Problema 13. *Demonstrar que a congruência* $6x^2 + 5x + 1 \equiv 0 \pmod{m}$ *tem solução para todo valor natural de* m.

Problema 14. *Demonstrar que existem infinitos primos da forma* $3k+1$ *e* $3k-1$.

Problema 15. *Demonstrar que se* $\mathrm{mdc}(a, b) = 1$ *o número* $a^2 + b^2$ *não pode ter fatores primos da forma* $4k - 1$ *e se além disso* $\mathrm{mdc}(a, 3) = 1$ *então o número* $a^2 + 3b^2$ *não pode ter fatores ímpares da forma* $3k - 1$. *Que podemos dizer sobre os fatores primos de* $a^2 + pb^2$ *onde* p *é um primo?*

Problema 16. *Demonstrar que, para* $p = 1093$,

$$2^{\frac{p-1}{2}} \equiv -1 \pmod{p^2}.$$

Problema 17. *a) (Euler) Seja* $F_n = 2^{2^n} + 1$ *o* n*-ésimo número de Fermat. Prove que todo fator primo de* F_n *é da forma* $k \cdot 2^{n+1} + 1$.

b) (Lucas) Prove que, se $n \geq 2$, *então todo fator primo de* F_n *é da forma* $k \cdot 2^{n+2} + 1$.

c) Mostre que $2^{2^5} + 1$ *é composto.*

Problema 18 (IMO1996)**.** *Sejam* a, b *inteiros positivos tais que* $15a + 16b$ *e* $16a - 15b$ *sejam quadrados perfeitos. Encontrar o menor valor que pode tomar o menor destes quadrados.*

Problema 19. *Seja* p *um número primo ímpar. Mostrar que o menor não resto quadrático positivo de* p *é menor que* $\sqrt{p} + 1$.

Problema 20. *Sejam* M *um número inteiro e* p *um número primo maior do que* 25. *Mostrar que a sequência* $M, M+1, \cdots, M+3\lfloor\sqrt{p}\rfloor - 1$ *contém um resto não quadrático módulo* p.

Problema 21 (Putnam 1991)**.** *Seja* p *um primo ímpar. Quantos elementos tem o conjunto*

$$\{x^2 \mid x \in \mathbb{Z}/p\mathbb{Z}\} \cap \{y^2 + 1 \mid y \in \mathbb{Z}/p\mathbb{Z}\}?$$

[Putnam 1991] Seja p *um primo ímpar. Quantos elementos tem o conjunto*

$$\{x^2 \mid x \in \mathbb{Z}/p\mathbb{Z}\} \cap \{y^2 + 1 \mid y \in \mathbb{Z}/p\mathbb{Z}\}?$$

Problema 22 (IMO2008)**.** *Prove que existe um número infinito de inteiros positivos* n *tais que* $n^2 + 1$ *tem um divisor primo maior do que* $2n + \sqrt{2n}$.

Dicas e Soluções

Em breve.

Referências

[1] F. E. Brochero Martinez, C. G. Moreira, N. C. Saldanha, E. Tengan - Teoria dos Números - um passeio com primos e outros números familiares pelo mundo inteiro, Projeto Euclides, IMPA, 2010.